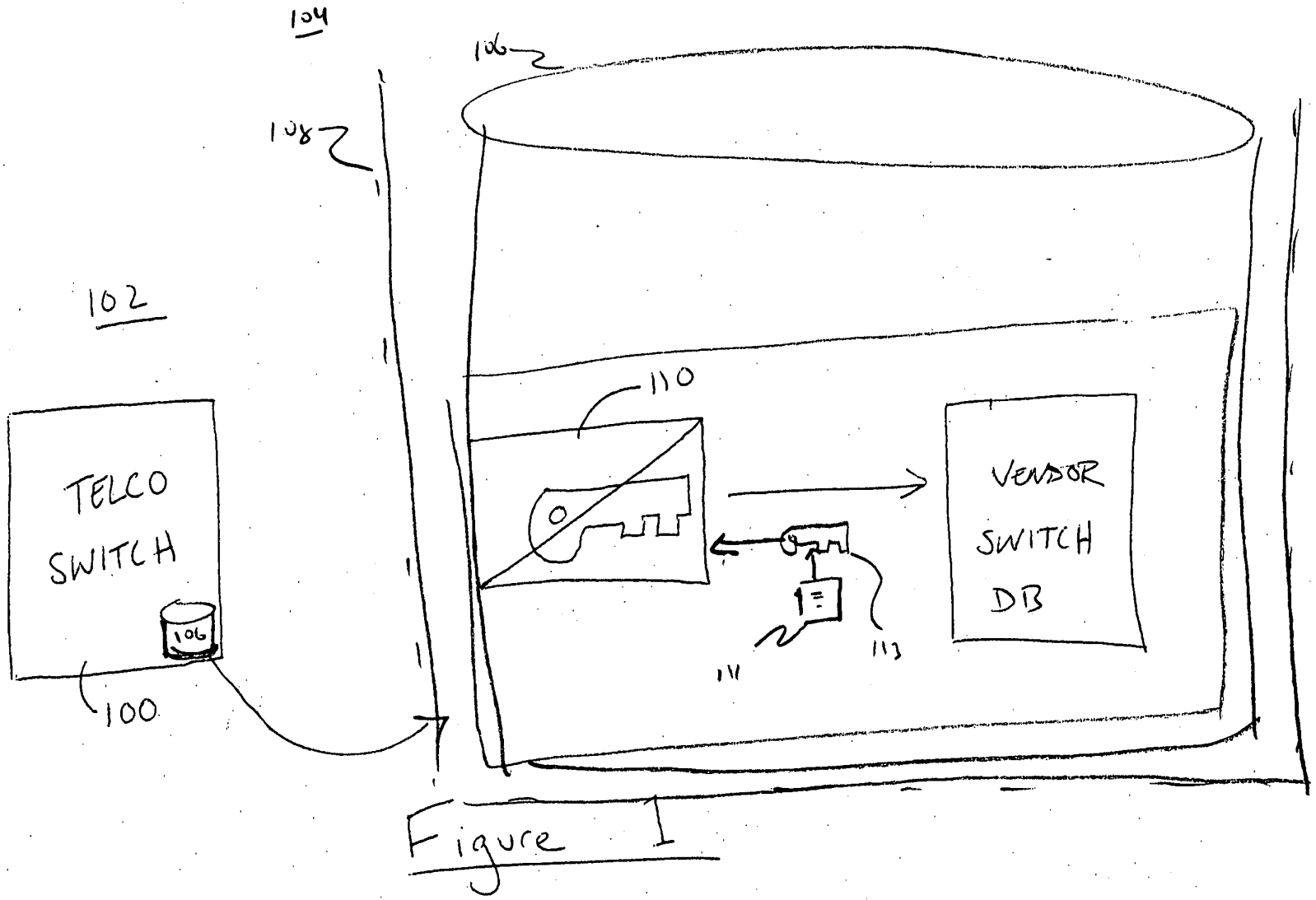
104
106
108
102
110
TELCO
SWITCH
106
100
VENDOR
SWITCH
DB
111
113

Figure 1

procedure 200 for the Telco

↓

Telco will define and retain the security in step 202.

↓

- MODLIOPT is executed in step 202a;

↓

- Type the Old Key → Type old key value step 202b
- <xxxxxxxxxxxx><CR>

↓

- Type the New Key → Type new key value step 202c
- <xxxxxxxxxxxx><CR>

↓

- Retype the New Key → Retype new key value step 202d
- <xxxxxxxxxxxx><CR>

↓

In step 202e the encrypted portion is Locked.

↓

In step 204, the Telco unlock the Security Lock.

- MODLIOPT: LOCK = OFF;

  Telco Types the Security Key in step 204a

↓

- <xxxxxxxxxxxx><CR>

↓

- Unlocked → Type the key value in 204b

Figure 2a

In step 206 the Telco unlocks the Security Lock after loading the COPYGEN.

- MODLIOPT: LOCK = OFF;

  Type the Security Key in step 206a

- <xxxxxxxxxxxx><CR>

  Unlocked → Type the key value in step 206b

In step 208 the Telco displays the Lock Status.

- DISPLIOPT;

  Locked is displayed → if the Security Lock is locked

  message is displayed in step 208a

  Unlocked is displayed → if the Security Lock is unlocked

  message is displayed in step 208b

Of course, other parameters that are administered using the MODLIOPT command may be displayed when DISPLIOPT is executed.

Figure 2b

an emergency procedure provided for the invention in step 210.

↓

The vendor performs an upgrade 210a

↓

authorized personnel are allowed to reset the Security Key to a new value in step 210b

↓

using the default key as the old value in step 210c.

↓

After the Security Key is reset, the authorized personnel enters the surveillance data in step 210d based on backup records, such as from paper or an equivalent recording method.

↓

Telco unlocks the Security Lock in step 212

↓

- MODLIOPT: LOCK = OFF;

  Type the Security Key in step 212a

↓

- <xxxxxxxxxxxx><CR>

  Unlocked → Type the key value in step 212b

↓

Telco may like to make it a practice in their operation procedure to define the Security Key to a new value after a new APS is loaded onto the switch in step 212c.

Figure 2c

The procedures 300 for the vendor are also provided by the invention as shown in Figure 3.

APS Upgrade Procedures for the vendor will now be explained in step 302.

For the first upgrade, there may be no surveillance information present as indicated by step 302a.

In this case, the vendor informs the Telco to define a new Security Key using the default key as the old key value instep 302b.

The vendor informs the Telco to unlock the Security Lock using the Security Key value in step 302c

allow their authorized personnel in step 302d to execute the display commands that cause the data to be displayed. These commands may be, for example, CALEA specific MML commands.

Figure 3a

In the case that the Vendor provides the security features in step 304,

the vendor informs the Telco in step 304a that the Security Key cannot be lost and cannot be made public.

The Telco is further advised that the Security Key should not be disclosed to even the vendor in step 304b.

The vendor informs the Telco that the only way to recover a lost Security Key is to re-perform the upgrade in step 304c.

In one aspect, the re-upgrade is done without the REGENerated commands. The Telco then defines a new Security Key in step 304d using the default key as the old value and enters the surveillance data based on records.

In step 306, the vendor advisee the Telco to unlock the Security Lock after reloading a COPYGEN.

Figure 3b

In step 308, the Upgrade Procedures from the vendor side

sequence number of the command is noted in step 308a and to be supplied to the Telco.

The Telco then executes in step 308b the DISPEACMD command to decrypt the MML commands for execution.

In step 308c, the encrypted CALEA specific MML commands from the log file are executed in the order they are entered into the log-file.

Figure 3c